

Dyrektor Generalny
Magdalena Maciejewska

Warszawa, 30.10.2019 r.

Dot. postępowania prowadzonego w trybie przetargu nieograniczonego pn. „Dostawa sprzętu i oprogramowania wraz z wdrożeniem do rozbudowy Platformy Usług Elektronicznych Urzędu Patentowego RP”, sygnatura postępowania: BG-II.211.23.2019

Wyjaśnienia i zmiana treści Specyfikacji Istotnych Warunków Zamówienia oraz zmiana terminu składania ofert

1. Działając na podstawie art. 38 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r. poz. 1843), zwanej dalej „ustawą”, Zamawiający udziela wyjaśnień na pytania wykonawców dotyczące treści specyfikacji istotnych warunków zamówienia (SIWZ) oraz na podstawie art. 38 ust. 4 ustawy dokonuje poniższych zmian w specyfikacji:

Pytanie nr 1

W załączniku nr 1 SOPZ w Rozdziale II „Gwarancja i wsparcie techniczne dla dostarczanego sprzętu” oraz w Rozdziale III „Gwarancja i wsparcie dla dostarczanego oprogramowania standardowego” Zamawiający definiuje wymagania w zakresie gwarancji i wsparcia dla sprzętu i oprogramowania. Prosimy o potwierdzenie, czy instancją Zamawiającego jest aby przedmiotowy, 5 letni okres gwarancji był opublikowany na oficjalnych stronach serwisowych producentów na dedykowanym dla Zamawiającego koncie produktowym?

Odpowiedź:

Zamawiający nie wymaga funkcjonalności publikacji okresu obowiązywania wsparcia technicznego/gwarancji na oficjalnym portalu w dedykowanym koncie Zakupowym, w wymaganym przez Zamawiającego zakresie jeśli Producent danego rozwiązania takich informacji nie udostępnia. Zamawiający wymaga natomiast spełnienia zapisów zawartych w Rozdziałach II i III.

Jednocześnie w ramach odpowiedzi na pytanie Zamawiający zmienia:

1. treść SOPZ (załącznik nr 1 do SIWZ) w poniższym zakresie:

a) Rozdział III Gwarancja i wsparcie dla dostarczanego oprogramowania standardowego

[ust. 1]

z:

[ust.1] Dostarczone Oprogramowanie standardowe musi być objęte 5 letnim (60 miesięcy) wsparciem technicznym producenta, liczonych od dnia podpisania przez obie Strony protokołu odbioru bez zastrzeżeń.

na:

[ust. 1] Dostarczone Oprogramowanie standardowe musi być objęte minimum 5 letnim (minimum 60 miesięcy) wsparciem technicznym producenta, liczonym od dnia podpisania przez obie Strony protokołu odbioru bez zastrzeżeń.

b) [tytuł]

z

Rozdział II Gwarancja i wsparcie techniczne dla dostarczanego sprzętu

na

Rozdział II Gwarancja i wsparcie techniczne dla dostarczanego sprzętu

oraz [ust. 1 i ust. 2]

z:

[ust. 1] Dostarczony Sprzęt musi być objęty 5 letnią (60 miesięcy) gwarancją producenta (która może być realizowana także przez podmioty autoryzowane przez producenta), liczoną od dnia podpisania przez obie Strony protokołu odbioru bez zastrzeżeń.

[ust. 2] Do obowiązków Wykonawcy należy zapewnienie 5 letniego (60 miesięcy) wsparcia technicznego dla dostarczonego sprzętu.

na:

[ust. 1] Dostarczony Sprzęt musi być objęty minimum 5 letnią (minimum 60 miesięcy) gwarancją producenta (która może być realizowana także przez podmioty autoryzowane przez producenta), liczoną od dnia podpisania przez obie Strony protokołu odbioru bez zastrzeżeń.

[ust. 2] Do obowiązków Wykonawcy należy zapewnienie *minimum* 5 letniego (*minimum* 60 miesięcy) wsparcia technicznego dla dostarczonego sprzętu.

oraz [ust. 11]

z:

[Ust. 11] Wykonawca gwarantuje sprawność i niezawodność wymienionego Sprzętu lub jego wymienionych części przez okres 5 lat od dnia podpisania protokołu z naprawy.

na:

[Ust. 11] Wykonawca gwarantuje sprawność i niezawodność wymienionego Sprzętu lub jego wymienionych części przez okres minimum 5 lat od dnia podpisania protokołu z naprawy.

2. postanowienia umowy (Załącznik nr 6 do SIWZ – Wzór umowy):

§ 8 Gwarancja

[ust. 1]

z:

[ust. 1] Wykonawca oświadcza, że udziela Zamawiającemu gwarancji producenta na Sprzęt i Oprogramowanie na zasadach opisanych poniżej, na okres 5 lat (60 miesięcy), począwszy od dnia podpisania Protokołu Odbioru Instalacji Sprzętu i Oprogramowania.

na;

[ust. 1] Wykonawca oświadcza, że udziela Zamawiającemu gwarancji producenta na Sprzęt i Oprogramowanie na zasadach opisanych poniżej, na okres minimum 5 lat (minimum 60 miesięcy), począwszy od dnia podpisania Protokołu Odbioru Instalacji Sprzętu i Oprogramowania.

oraz [ust. 18]

z:

[ust. 18] Wykonawca gwarantuje sprawność i niezawodność wymienionego Sprzętu lub jego wymienionych części przez okres 5 lat od dnia podpisania przez Zamawiającego Protokołu Z Naprawy. Wzór Protokołu z Naprawy stanowi Załącznik Nr 9 do Umowy.

na:

[ust. 18] Wykonawca gwarantuje sprawność i niezawodność wymienionego Sprzętu lub jego wymienionych części przez okres minimum 5 lat od dnia podpisania przez Zamawiającego Protokołu Z Naprawy. Wzór Protokołu z Naprawy stanowi Załącznik Nr 9 do Umowy.

oraz [ust. 21]

z:

[ust. 21] Dostarczone Oprogramowanie musi być objęte 5 letnim (60 miesięcy) wsparciem technicznym producenta, liczonym od dnia rozpoczęcia gwarancji.

na:

[ust. 21] Na Dostarczone Oprogramowanie musi być objęte minimum 5 letnim (minimum 60 miesięcy) wsparciem technicznym producenta, liczonym od dnia rozpoczęcia gwarancji.

Pytanie nr 2

Prosimy o potwierdzenie, czy elementy wyspecyfikowane przez Zamawiającego w załączniku nr 1 SOPZ w rozdziale IX ust. 3 w zakresie gwarancji powinny być realizowane zgodnie z zapisami zawartymi w Rozdziale II i III przedmiotowego załącznika?

Odpowiedź:

Zamawiający potwierdza, że elementy wyspecyfikowane przez Zamawiającego w załączniku nr 1 SOPZ w rozdziale IX ust. 3 w zakresie gwarancji powinny być realizowane zgodnie z zapisami zawartymi w Rozdziale II i III przedmiotowego załącznika.

Pytanie nr 3

Prosimy o potwierdzenie, czy w zakresie spełnienia wymagania zdefiniowanego przez Zamawiającego w załączniku nr 1 SOPZ w rozdziale IX ust. 3 w tabeli w wierszu nr 2, Zamawiający dopuści rozwiązanie, które posiada średnią przepustowość filtrowania ruchu http/https minimum 200Mbps jednakże dla ruchu http posiada przepustowość minimum 250Mbps a dla ruchu https posiada przepustowość minimum 150Mbps?

Odpowiedź:

Zamawiający nie dopuści rozwiązania, które posiada średnią przepustowość filtrowania ruchu http/https minimum 200Mbps jednakże dla ruchu http posiada przepustowość minimum 250Mbps a dla ruchu https posiada przepustowość minimum 150Mbps. Zamawiający oczekuje rozwiązania które, będzie filtrować ruch zarówno http i https o przepustowości minimum 200Mbps.

Pytanie nr 4

Prosimy o potwierdzenie, czy w zakresie spełnienia wymagania zdefiniowanego przez Zamawiającego w załączniku nr 1 SOPZ w rozdziale IX ust. 3 w tabeli w wierszu nr 10, Zamawiający dopuści rozwiązanie równoważne, gdzie tryb autouczenia jest zastąpiony uczeniem maszynowym, które na bieżąco sprawdza zgodność wartości parametrów z modelem statystycznym oraz wychwycone anomalie ocenia pod kątem stopnia zagrożenia?

Pozytywny model bezpieczeństwa obejmuje:

- Ochrona przed CSRF.
- Ochrona AntiDeface.
- Nagłówki http.
- Źródłowy adres IP.
- Identyfikator sesji lub nazwy użytkownika.
- Ilość wystąpień w określonym przez administratora czasie, elementy aplikacji (url-e, parametry), nazwa aplikacji klienta.
- Ochrona przed użyciem skompromitowanych baz użytkowników w celu logowania - Credential Stuffing Defense Service.
- Wykrywanie nielegalnego formatu JSON.
- Walidacja zgodności XML ze schematem.

- Ochrona przed clickjackeim.
- Przejścia pomiędzy URL-ami.
- Ochrona cookie.
- Content Type.
- Kody odpowiedzi http.
- Ochrona przed atakami Man in the Browser.
- Reguły ograniczeń protokołu http: Content Length, http header lenght, name, value, http parameter properties, http request properties, http/2 frame properties, zgodność z RFC.

Nadmienić należy, że różni producenci w różny sposób realizują funkcję celu, a każde z przedmiotowych rozwiązań w efekcie końcowym daje taki sam efekt końcowy.

Odpowiedź:

W ramach odpowiedzi na pytanie Zamawiający zmienia treść SOPZ (załącznik nr 1 do SIWZ) w poniższym zakresie:

Rozdział IX ust. 3

[tabela, wiersz 10]

z:

Oferowane rozwiązanie musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie uczenia maszynowego lub automatycznie budowany przez WAF profil aplikacji Web. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:

- wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URLa.
- typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT),
- przejścia pomiędzy URL-ami (servletami),
- dopuszczalne metody http,
- dopuszczalne cookie,
- parametry dynamiczne,
- typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany),
- dopuszczalne parametry w danym servlecie,
- długość zapytań,
- nazwy hosta,
- wystąpień i długość parametrów (per każdy parametr),
- wystąpień i długości nagłówków,
- wystąpień i długości cookies,
- oczekiwanych typów znaków per każdy parametr,
- typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku,
- URL-i podatnych na CSRF

na:

Oferowane rozwiązanie musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie uczenia maszynowego lub automatycznie budowany przez WAF profil aplikacji Web.

Pytanie nr 5

Prosimy o potwierdzenie, czy w zakresie spełnienia wymagania zdefiniowanego przez Zamawiającego w załączniku nr 1 SOPZ w rozdziale IX ust. 3 w tabeli w wierszu nr 11 oraz 12, Zamawiający dopuści rozwiązanie równoważne, gdzie wskazywane są strony logowania oraz zapewniona jest ochrona przed Session Fixation oraz Credential Stuffing (użycie skradzionych poświadczeń), a oprócz ochrony sygnaturowej aplikacji web dodatkowo zapewniona jest ochrona antywirusowa przy współpracy z sandboxem w chmurze producenta?

Odpowiedź:

W ramach odpowiedzi na pytanie Zamawiający zmienia treść SOPZ (załącznik nr 1 do SIWZ) w poniższym zakresie:

Rozdział IX ust. 3

[tabela, wiersz 12]

z:

Oferowane rozwiązanie musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.

na:

Oferowane rozwiązanie musi posiadać funkcjonalność ochrony stron logowania użytkowników.

Pytanie nr 6

Prosimy o potwierdzenie, czy w zakresie spełnienia wymagania zdefiniowanego przez Zamawiającego w załączniku nr 1 SOPZ w rozdziale IX ust. 3 w tabeli w wierszu nr 11 oraz 12, Zamawiający dopuści rozwiązanie, które umożliwia odtworzenie firmaware i konfiguracji z GUI lub z CLI przez TFTP?

Odpowiedź:

W ramach odpowiedzi na pytanie Zamawiający zmienia treść SOPZ (załącznik nr 1 do SIWZ) w poniższym zakresie:

Rozdział IX ust. 3

[tabela, wiersz 18]

z:

Oferowane rozwiązanie musi posiadać możliwość pełnego odtworzenia konfiguracji oprogramowania i systemu operacyjnego z nośnika USB.

na:

Oferowane rozwiązanie musi posiadać możliwość pełnego odtworzenia konfiguracji oprogramowania i systemu operacyjnego.

Pytanie nr 7

W Załączniku nr 1 SOPZ w rozdziale X ust. 4 w tabeli w wierszu nr 31, Zamawiający wymaga aby cyt. „Oprogramowanie wraz z niezbędnymi licencjami musi posiadać aktywne wsparcie Producenta zgodnie z zapisami zawartymi w Rozdziale III.”. Z uwagi, iż firma Microsoft prowadzi politykę sprzedażową, wg. której istnieje możliwość zakupu przedmiotowego wsparcia na okres tylko 2 lat lub całkowitej wielokrotności tej wartości, zwracamy się do Zamawiającego z pytaniem czy wyrazi zgodę na zmianę przedmiotowego wymogu na okres 4 lat lub 6 lat?

Odpowiedź:

Zamawiający udzielił odpowiedzi na zadane pytanie udzielając odpowiedzi na pytanie nr 1.

Pytanie nr 8

Zamawiający wymaga, aby oferowane rozwiązanie umożliwiała przejścia pomiędzy URL-ami (servletami). Przejścia pomiędzy URL-ami (servletami) są wbudowane w same aplikacje webowe i nie ma potrzeby używania do tego rozwiązania WAF. Istnieje ryzyko zablokowania strony kiedy użytkownik wpisuje ręcznie adres URL, a także może powodować blokowanie pozytywnych BOTów przeszukujących naszą stronę, np. Google Bot. Dlatego bardzo mała ilość rozwiązań WAF posiada taką funkcjonalność, a nawet jeśli już jest to nie jest ona uruchamiana/używana. W związku z powyższym czy Zamawiający zgadza się na wykreślenie tego zapisu?

Odpowiedź:

Zamawiający udzielił odpowiedzi na zadane pytanie udzielając odpowiedzi na pytanie nr 4.

Pytanie nr 9

Zamawiający wymaga, aby oferowane rozwiązanie posiadało funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznego włączania dla tych stron ochrony przed atakami brute force. W celu prawidłowego zabezpieczenia stron logowania przed atakami brute force, należy znać aplikację, którą chronimy wraz z informacjami jakie kody oraz informacje są przesyłane z aplikacji w przypadku udanego i nieudanego logowania. System sam nie jest w stanie rozróżnić kiedy użytkownik został poprawnie zalogowany, a kiedy logowanie się nie powiodło. Strona logowania jest krytycznym punktem aplikacji i zazwyczaj pojawia się tylko jedna per aplikacja, dlatego najlepiej zabezpieczyć taką stronę w sposób manualny. W związku z powyższym czy Zamawiający zgodzi się na wykreślenie tego zapisu?

Odpowiedź:

Zamawiający udzielił odpowiedzi na zadane pytanie udzielając odpowiedzi na pytanie nr 5.

Pytanie nr 10

Zamawiający wymaga, aby oferowane rozwiązanie w czasie i po wykonaniu upgrade'u wersji oprogramowania lub po instalacji łatki (patcha) umożliwiało cofnięcie jego wersji oprogramowania do poprzedniej bez konieczności reinstalacji oprogramowania z nośników zewnętrznych o ile producent umożliwia taką operację dla konkretnej poprawki. Samo cofnięcie wersji oprogramowania do poprzedniej jest bardzo często możliwe, natomiast problem jest z konfiguracją, która często przy cofnięciu wymaga odtworzenia z backup'u. Czy Zamawiający dopuszcza możliwość przywrócenia konfiguracji z backup'u w przypadku cofnięcia wersji oprogramowania do poprzedniej bez konieczności reinstalacji oprogramowania z nośników zewnętrznych o ile producent umożliwia taką operację dla konkretnej poprawki?

Odpowiedź:

Zamawiający dopuszcza możliwość przywrócenia konfiguracji z backup'u w przypadku cofnięcia wersji oprogramowania do poprzedniej bez konieczności reinstalacji oprogramowania z nośników zewnętrznych o ile producent umożliwia taką operację dla konkretnej poprawki.

3. Działając na podstawie art. 38 ust. 6 ustawy Zamawiający przedłuża termin składania ofert do dnia **13 listopada 2019 r. do godz. 11:00.**

Otwarcie ofert nastąpi 13 listopada 2019 r. o godz. 11.30 w siedzibie Zamawiającego, w pokoju nr 205.

DYREKTOR GENERALNY
Urzędu Patentowego Rzeczypospolitej Polskiej
Magdalena Maciejewska /-/